Yee & Associates, P.C.

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner Kambiz Zand** **Group Art Unit 2132**	Facsimile No.: **571/273-8300**
From: Amelia Turner Legal Assistant to Lisa L.B. Yociss	No. of Pages Including Cover Sheet: **27**

Message:

Transmitted herewith:

- Transmittal of Appeal Brief; and
- Appeal Brief.

Re: Application No.: **09/874,649**
Attorney Docket No: **2001-025-SFT**

Date: Monday, February 13, 2006

Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

RECEIVED
CENTRAL FAX CENTER
FEB 13 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **McCown et al.**

Serial No.: **09/874,649**

Filed: **June 5, 2001**

For: **Anti-Piracy Network Storage Device**

§ Group Art Unit: **2132**

§ Examiner: **Zand, Kambiz**

§ Attorney Docket No.: **2001-025-SFT**

§

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300, on February 13, 2006.

By: Amelia C. Turner

51344
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

TRANSMITTAL OF APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
TRANSMITTED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37)

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to Yee & Associates, P.C. Deposit Account No. 50-3157. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to Yee & Associates, P.C. Deposit Account No. 50-3157. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to Yee & Associates, P.C. Deposit Account No. 50-3157.

Respectfully submitted,

Lisa L.B. Yociss
Registration No. 36,975

Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEYS FOR APPLICANTS

RECEIVED
CENTRAL FAX CENTER
FEB 13 2006

PATENT

Docket No. 2001-025-SFT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **McCown et al.**	§	
	§	Group Art Unit: **2132**
Serial No. **09/874,649**	§	
	§	Examiner: **Zand, Kambiz**
Filed: **June 5, 2001**	§	
	§	
For: **Anti-Piracy Network Storage Device**	§	
	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300, on February 13, 2006.

By: Amelia C. Turner
Amelia C. Turner

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on December 12, 2005.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

02/15/2006 LWONDIM1 00000077 503157 09874649

01 FC:1402 500.00 DA

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: Storage Technology Corporation, as reflected in the Assignment recorded on June 5, 2001, at Reel 011901, Frame 0352.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-3, 5-14, 16-21, 23-33, and 35-50.

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 4, 15, 22, and 34.
2. Claims withdrawn from consideration but not canceled: None.
3. Claims pending: 1-3, 5-14, 16-21, 23-33, and 35-50.
4. Claims allowed: None.
5. Claims rejected: 1-3, 5-14, 16-21, 23-33, and 35-50.
6. Claims objected to: None.

C. CLAIMS ON APPEAL

The claims on appeal are: 1-3, 5-14, 16-21, 23-33, and 35-50.

STATUS OF AMENDMENTS

A Response to Final Rejection was transmitted on November 14, 2005.

SUMMARY OF CLAIMED SUBJECT MATTER

Applicants' independent claim 1 describes a method of transmitting data in a network (specification page 5, lines 3-18) comprising: receiving from a client a request to transmit the data; encrypting the data; and transmitting the encrypted data to a storage device, that is associated with the client, connected to the network, the client being incapable of decrypting the encrypted data, wherein unencrypted transmission of the data through the client is bypassed. (Specification page 7, lines 11-14, page 11, lines 13-16 and 29-30, page 12, lines 6-10, and page 15, lines 18-29.)

Applicants' independent claim 13 describes a method, operative in a storage device that is associated with a client, of downloading data from a server in response to a client request from the client (specification page 5, lines 3-18 and page 10, lines 12-22), comprising: receiving from the server a request for downloading; receiving an encrypted data transmission from the server; the client being incapable of decrypting the encrypted data; decrypting the encrypted data transmission to yield the data; and storing the data in the storage device. (Specification page 7, lines 11-14, page 11, lines 13-16 and 29-30, page 12, lines 6-10, and page 16, lines 1-7.)

Applicants' independent claim 19 describes a computer program product in a computer-readable medium for transmitting data in a network (specification page 5, lines 3-18 and page 16, lines 8-27), comprising instructions for: receiving from a client a request to transmit the data; encrypting the data; and transmitting the encrypted data to a storage device, that is associated with the client, connected to the network, the client being incapable of decrypting the encrypted data, wherein unencrypted transmission of the data through the client is bypassed. (Specification page 7, lines 11-14, page 11, lines 13-16 and 29-30, page 12, lines 6-10, and page 15, lines 18-29.)

Applicants' independent claim 31 describes an embedded processor program in an embedded processor-readable medium and operative in a storage device that is associated with a client, of downloading data from a server in response to a client request from the client (specification page 5, lines 3-18 and page 10, lines 12-22), comprising instructions for: receiving from the server a request for downloading; receiving an encrypted data transmission from the

server; the client being incapable of decrypting the encrypted data; decrypting the encrypted data transmission to yield the data; and storing the data in the storage device. (Specification page 7, lines 11-14, page 11, lines 13-16 and 29-30, page 12, lines 6-10, and page 15, lines 1-7.)

Applicants' independent claim 42 describes a data processing system for transmitting data in a network, comprising: a bus system; a processing unit connected to the bus system, wherein the processing unit includes at least one processor; memory connected to the bus system; a network adapter in communication with the network and with the bus system; and a set of instructions in the memory (specification page 5, lines 3-18 and page 10, lines 12-22), wherein the processing unit executes the set of instructions to perform the acts of: receiving with the network adapter and from a client a request to transmit the data; encrypting the data; and transmitting the encrypted data to a storage device, that is associated with the client, connected to the network, the client being incapable of decrypting the encrypted data, wherein unencrypted transmission of the data through the client is bypassed. (Specification page 7, lines 11-14, page 11, lines 13-16 and 29-30, page 12, lines 6-10, and page 15, lines 18-29.)

Applicants' independent claim 44 describes a storage device, that is associated with a client, for downloading data from a server in response to a client request from the client, comprising: a bus system; an embedded processor unit connected to the bus system, wherein the embedded processor includes at least one embedded processor; memory connected to the bus system; a network adapter connected to the bus system; physical storage components in communication with the bus system; and a set of instructions in the memory (specification page 5, lines 3-18 and page 10, lines 12-22), wherein the embedded processor unit executes the set of instructions to perform the acts of: receiving with the network adapter and from the server a request for downloading; receiving an encrypted data transmission from the server; the client being incapable of decrypting the encrypted data; decrypting the encrypted data transmission to yield the data; and storing the data, in the storage device, with the physical storage components. (Specification page 7, lines 11-14, page 11, lines 13-16 and 29-30, page 12, lines 6-10, and page 16, lines 1-7.)

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1-3, 5-14, 16-21, 23-33, and 35-50)

Claims 1-3, 5-14, 16-21, 23-33, and 35-50 stand finally rejected under 35 U.S.C. § 112, second paragraph.

B. GROUND OF REJECTION 2 (Claims 1-3, 5-14, 16-21, 23-33, and 35-50)

Claims 1-3, 5-14, 16-21, 23-33, and 35-5 stand finally rejected under 35 U.S.C. § 112, first paragraph.

C. GROUND OF REJECTION 3 (Claims 1-3, 5-14, 16-21, 23-33, and 35-50)

Claims 1-3, 5-14, 16-21, 23-33, and 35-50 stand finally rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent 6,005,969 issued to *Fortenberry*.

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-3, 5-14, 16-21, 23-33, and 35-50)

Claims 1-3, 5-14, 16-21, 23-33, and 35-50 stand finally rejected under 35 U.S.C. § 112, second paragraph. This position is not well founded.

The Examiner included a heading in the Final Office Action mailed September 12, 2205, that reads "Claim Rejections – 35 U.S.C. § 112". Under this heading, the Examiner included a quotation of the first paragraph of 35 U.S.C. § 112. The Examiner then rejected claims 1-3, 5-14, 16-21, 23-33, and 35-50 under U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. However, no explanation whatsoever is provided by the Examiner of the deficiency of these claims. This position is not well founded and should be reversed because the Examiner has provided no explanation as to a believed deficiency of the claims.

B. GROUND OF REJECTION 2 (Claims 1-3, 5-14, 16-21, 23-33, and 35-50)

Claims 1-3, 5-14, 16-21, 23-33, and 35-5 stand finally rejected under 35 U.S.C. § 112, first paragraph. This position is not well founded.

Specifically, the Examiner stated that the limitation "the client being incapable of decrypting the encrypted data" has no support in the specification.

The specification states that the server contacts the storage device directly. See specification page 7, lines 11-14. The server sends the data over the communications channel directly to the network storage device 108. See specification page 7, lines 11-14. Figure 3 depicts the operation of a secure sockets layer (SSL) communication between the storage device and the server. An SSL connection is maintained between the storage device and the server. See specification page 11, lines 13-16. SSL relies on public key cryptography. See specification page 11, line 29. "In a public key cryptosystem, the parties exchange public keys, but keep the private keys secret. In this way, each of the parties can encrypt messages to send to the other party, and only the intended recipient will be able to decrypt the message." Specification page 12, lines 6-10.

Applicants' specification explicitly states that only the parties that have possession of the keys can decrypt messages that were encrypted using these keys. See specification page 12, lines

6-10. The server and storage device use SSL to communicate. Thus, Applicants' specification teaches that only the server and storage device can decrypt encrypted data that is transmitted between the server and storage device using SSL where only the server and storage device have possession of the keys used to encrypt the data. Because the client is not the intended recipient, the client is incapable of decrypting encrypted data that is transmitted between the server and storage device because the client is not in possession of the keys. Therefore, Applicants' specification complies with the written description requirement because the limitation "the client being incapable of decrypting the encrypted data" is supported in the specification.

C. GROUND OF REJECTION 3 (Claims 1-3, 5-14, 16-21, 23-33, and 35-50)

Claims 1-3, 5-14, 16-21, 23-33, and 35-50 stand finally rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent 6,005,969 issued to *Fortenberry*. This position is not well founded.

The Examiner stated that, for purposes of examination, the Examiner considered the limitation of "the client being incapable of decrypting the encrypted data" as corresponding to "a client not being able to decrypt an encrypted data unless the client possesses the decryption key". Applicants' claimed features are not equivalent and do not correspond to the language used by the Examiner. The Examiner has interpreted Applicants' claims by substituting completely different concepts for the wording of Applicants' claims which has fundamentally changed the meaning of the claims.

Applicants' claim 1 is exemplary of the other independent claims. Applicants' claim 1 describes receiving from a client a request to transmit the data, encrypting the data, and transmitting the encrypted data to a storage device, that is associated with the client, connected to the network, the client being incapable of decrypting the encrypted data, wherein unencrypted transmission of the data through the client is bypassed. Applicants claim "the client being incapable of decrypting the encrypted data" in the independent claims. The Examiner has disregarded the language of Applicants' claims and instead substituted completely different language.

Applicants claim the client being incapable of decrypting particular data. This is the same data that was encrypted, as described earlier in the claim, as being requested by the client.

After the client requested this particular data, it was encrypted. This encrypted data is then transmitted to a storage device. It is this encrypted data that the client is incapable of decrypting.

By substituting the generic statement, "a client not being able to decrypt an encrypted data unless the client possesses the decryption key", in place of Applicants' much more specific feature, the Examiner has broaden Applicants' claims beyond what is actually claimed by Applicants. According to the language used by the Examiner, the data that the client is unable to encrypt is not any specific data. It is certainly not the particular data claimed by Applicants.

Applicants do not claim a client not being able to decrypt some random data. According to Applicants' claims, the data that the client is unable to decrypt is specifically described earlier in the claims. The data the client is unable to decrypt is that data that was requested by the client and that was then encrypted.

The Examiner has interpreted Applicants' claims using language that is not equivalent to and does not correspond to the language included in Applicants' claims.

The Examiner also stated that "applicant's passing the unencrypted transmission corresponds to transmission of the encrypted data between the two entities using a secure channel of communication". Applicants claim "wherein unencrypted transmission of the data through the client is bypassed". The Examiner has again disregarded Applicants' claim language and used, instead, language that does not correspond to the language of Applicants' claims.

Applicants' actual claim language means that an unencrypted transmission of the data does not occur through the client. This is not at all the same as transmitting encrypted data between two entities using a secure channel of communication. Applicants refer to specific "data" in this feature. This is the data that was encrypted and then transmitted to a storage device that is associated with the client and connected to the network. Applicants do not claim merely encrypted transmissions using a secure channel of communication.

Further, just because unencrypted transmission is bypassed does not mean that two entities are communicating using a secure channel of communication. The Examiner has interpreted Applicants' claims by substituting completely different concepts for the wording of Applicants' claims which has fundamentally changed the meaning of the claimed feature.

Regarding the art that the Examiner cites as anticipating Applicants' claims, *Fortenberry* does not anticipate Applicants' claims because *Fortenberry* does not teach the client being incapable of decrypting the encrypted data wherein unencrypted transmission of the data through

the client is bypassed, and *Fortenberry* does not teach a storage device that is associated with the client.

Fortenberry teaches a user sending a request to a passport agent. The passport agent then transmits information about that user to a web site. The request from the user to the passport agent is encrypted. Before the passport agent sends the information about the user to the web site, the passport agent encrypts the information. The passport agent then sends encrypted data to the web site. The user provides a key to the web site for the web site to use to decrypt the information. Thus, the user is capable of decrypting the encrypted information because the user holds the key that is needed in order to be able to decrypt the encrypted data.

The Examiner stated that the Examiner considers the "user" taught by *Fortenberry* as corresponding to Applicants' "client". As discussed above, the "user" taught by *Fortenberry* is capable of decrypting the encrypted information. Therefore, *Fortenberry* does not anticipate Applicants' claims because *Fortenberry* does not describe the client being incapable of decrypting the encrypted data wherein unencrypted transmission of the data through the client is bypassed.

The Examiner stated that column 6, lines 16-46, of *Fortenberry* teaches "the client being incapable of decrypting the encrypted data". The cited section of *Fortenberry* teaches the user requesting that the passport agent release specific user information to the web site. This request is then encrypted. The passport agent is provided with a key with which to decrypt the encrypted message sent by the user. The user can decrypt the encrypted message that includes the request because it is the user that encrypted the message.

This section also describes the passport agent transmitting encrypted data to the web site. The user can decrypt the encrypted data because *Fortenberry* states at lines 26-29, "user 208 has previously provided to web site 210 a public key with which web site 210 can decode the encrypted data provided by passport agent". The user can decrypt the encrypted data because the user is the one that provided the key to use to decrypt the encrypted data.

Fortenberry states at lines 30-36, "the web site 210 receives the encrypted user information (i.e. the passport) from passport agent 216 and unlocks the message using the public key provided by the user 208". The user can decrypt the encrypted user information because the user is the one that provided the key to use to decrypt the encrypted user information.

Fortenberry further emphasizes, at lines 36-38, that it is the user that can decrypt the encrypted information by stating that "user 208 can provide to web site 210 one of several public keys which allow web site 210 to unlock data having one of several security levels".

The section cited by the Examiner, column 6, lines 16-46, states that it is the user that provides the key to decrypt the encrypted data. The user is able to decrypt the data because the user has the key. Therefore, the section cited by the Examiner teaches that the user is capable of decrypting the encrypted data. Therefore, *Fortenberry* does not anticipate Applicants' claims because *Fortenberry* does not describe the client being incapable of decrypting the encrypted data wherein unencrypted transmission of the data through the client is bypassed.

Applicants also claim the storage device being associated with the client. In *Fortenberry*, the web site is not associated with the user. In fact, *Fortenberry* teaches away from the web site being associated with the user because according to *Fortenberry*, the user wishes to keep the user's identity secret from the web site. See column 2, lines 17-20. Since *Fortenberry* does not teach the web site being associated with the user, *Fortenberry* does not anticipate Applicants' claims.

Fortenberry teaches away from Applicants' claims. Applicants claim the client being incapable of decrypting the encrypted data wherein unencrypted transmissions of the data through the client is bypassed. *Fortenberry* teaches a passport agent that transmits encrypted data to the web site. The passport agent encrypts the data. The passport agent assigns an encryption key based on the user's password. The password agent then provides the public key to the user. This public key is required in order to be able to decrypt the encrypted data.

The user then provides the web site with this key for the web site to use to decrypt the encrypted data. Thus, *Fortenberry* teaches the user being able to decrypt the encrypted data that is transmitted from the passport agent to the web site because the user provides the key to use for decryption. If the user does not provide the proper key for the web site to use to decrypt the data, the web site will not be able to decrypt the data. Therefore, *Fortenberry* does not teach the client being incapable of decrypting the encrypted data. *Fortenberry* expressly teaches the user being able to decrypt the data. Because *Fortenberry* does not teach the client being incapable of decrypting the encrypted data, *Fortenberry* does not anticipate Applicants' claims and actually teaches away from Applicants' claims.

The remaining claims depend from the independent claims that describe a storage device that is associated with the client and the client being incapable of decrypting the encrypted data wherein unencrypted transmission of the data through the client is bypassed. Thus, the remaining claims are believed to be patentable because *Fortenberry* does not teach the features of the dependent claims in combination with the storage device being associated with the client and the client being incapable of decrypting the encrypted data.

D. CONCLUSION

Fortenberry does not anticipate Applicants' claims because *Fortenberry* does not teach the client being incapable of decrypting the encrypted data wherein unencrypted transmission of the data through the client is bypassed, or a storage device that is associated with the client.

Therefore, Applicants' claims are believed to be patentable over the cited prior art.

Lisa L.B. Yociss
Reg. No. 36,975
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal reads:

1. A method of transmitting data in a network comprising:

receiving from a client a request to transmit the data;

encrypting the data; and

transmitting the encrypted data to a storage device, that is associated with the client, connected to the network, the client being incapable of decrypting the encrypted data, wherein unencrypted transmission of the data through the client is bypassed.

2. The method of claim 1, further comprising:

negotiating encryption parameters.

3. The method of claim 2, wherein the step of negotiating encryption parameters includes establishing an encrypted communications channel.

5. The method of claim 1, wherein the data includes at least one of audio data, video data, and digital data.

6. The method of claim 1, wherein the storage device stores the data in a removable medium.

7. The method of claim 6, wherein the removable medium is one of a compact disc (CD) and a digital versatile disc (DVD).

8. The method of claim 6, wherein the removable medium is one of a tape cartridge and a tape cassette.

9. The method of claim 6, wherein the removable medium is one of a holographic disc and a holographic cube.

10. The method of claim 1, wherein the storage device is one of a tape drive and a disk drive.

11. The method of claim 1, wherein the storage device is a solid-state storage device.

12. The method of claim 1, wherein the storage device is independent of the client.

13. A method, operative in a storage device that is associated with a client, of downloading data from a server in response to a client request from the client:
receiving from the server a request for downloading;
receiving an encrypted data transmission from the server;
the client being incapable of decrypting the encrypted data;
decrypting the encrypted data transmission to yield the data; and
storing the data in the storage device.

14. The method of claim 13, further comprising negotiating encryption parameters.

16. The method of claim 13, wherein the data includes at least one of audio data, video data and digital data.

17. The method of claim 13, wherein the storage device is a compact disc writer.

18. The method of claim 13, wherein the storage device is one of a tape drive and a disk drive.

19. A computer program product in a computer-readable medium for transmitting data in a network, comprising instructions for:
receiving from a client a request to transmit the data;
encrypting the data; and
transmitting the encrypted data to a storage device, that is associated with the client, connected to the network, the client being incapable of decrypting the encrypted data, wherein unencrypted transmission of the data through the client is bypassed..

20. The computer program product of claim 19, comprising additional instructions for:
negotiating encryption parameters.

21. The computer program product of claim 20, wherein the instructions for negotiating encryption parameters include instructions for establishing an encrypted communications channel.

23. The computer program product of claim 19, wherein the data includes at least one of audio data, video data, and digital data.

24. The computer program product of claim 19, wherein the storage device stores the data in a removable medium.

25. The computer program product of claim 24, wherein the removable medium is one of a compact disc (CD) and a digital versatile disc (DVD).

26. The computer program product of claim 24, wherein the removable medium is one of a tape cartridge and a tape cassette.

27. The computer program product of claim 24, wherein the removable medium is one of a holographic disc and a holographic cube.

28. The computer program product of claim 19, wherein the storage device is one of a tape drive and a disk drive.

29. The computer program product of claim 19, wherein the storage device is a solid-state storage device.

30. The computer program product of claim 19, wherein the storage device is independent of the client.

31. An embedded processor program in a embedded processor-readable medium and operative in a storage device that is associated with a client, of downloading data from a server in response to a client request from the client, comprising instructions for:
receiving from the server a request for downloading;
receiving an encrypted data transmission from the server;
the client being incapable of decrypting the encrypted data;
decrypting the encrypted data transmission to yield the data; and
storing the data in the storage device.

32. The embedded processor program of claim 31, further comprising instructions for:
negotiating encryption parameters.

33. The embedded processor program of claim 32, wherein the instructions for negotiating encryption parameters include instructions for establishing an encrypted communications channel.

35. The embedded processor program of claim 31, wherein the data includes at least one of audio data, video data, and digital data.

36. The embedded processor program of claim 31, wherein the storage device stores the data in a removable medium.

37. The embedded processor program of claim 36, wherein the removable medium is one of a compact disc (CD) and a digital versatile disc (DVD).

38. The embedded processor program of claim 24, wherein the removable medium is one of a tape cartridge and a tape cassette.

39. The embedded processor program of claim 24, wherein the removable medium is one of a holographic disc and a holographic cube.

40. The embedded processor program of claim 31, wherein the storage device is one of a tape drive and a disk drive.

41. The embedded processor program of claim 31, wherein the storage device is a solid state storage device.

42. A data processing system for transmitting data in a network, comprising:

a bus system;

a processing unit connected to the bus system, wherein the processing unit includes at least one processor;

memory connected to the bus system;

a network adapter in communication with the network and with the bus system; and

a set of instructions in the memory,

wherein the processing unit executes the set of instructions to perform the acts of:

receiving with the network adapter and from a client a request to transmit the data;

encrypting the data; and

transmitting the encrypted data to a storage device, that is associated with the client, connected to the network, the client being incapable of decrypting the encrypted data, wherein unencrypted transmission of the data through the client is bypassed.

43. The data processing system of claim 42, wherein the storage device is independent of the client.

44. A storage device, that is associated with a client, for downloading data from a server in response to a client request from the client, comprising:

a bus system;

an embedded processor unit connected to the bus system, wherein the embedded processor includes at least one embedded processor;

memory connected to the bus system;

a network adapter connected to the bus system;

physical storage components in communication with the bus system; and

a set of instructions in the memory,

wherein the embedded processor unit executes the set of instructions to perform the acts of:

receiving with the network adapter and from the server a request for downloading;

receiving an encrypted data transmission from the server;

the client being incapable of decrypting the encrypted data;

decrypting the encrypted data transmission to yield the data; and

storing the data, in the storage device, with the physical storage components.

45. The storage device of claim 44, wherein the physical storage components store the data to a removable medium.

46. The storage device of claim 44, wherein the removable medium is one of a compact disc and a digital versatile disc (DVD).

47. The storage device of claim 44, wherein the removable medium is one of a tape cartridge and a tape cassette.

48. The storage device of claim 44, wherein the removable medium is one of a holographic disc and a holographic cube.

49. The storage device of claim 44, wherein the physical storage components store the data to one of tape and a disk.

50. The storage device of claim 44, wherein the physical storage components store the data to a solid-state device.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.